REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is either anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 542-7800 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Specification amendments

A single amendment has been made to the specification to correct a minor typographical error.

Status of claims

To simplify amending the claims and hence expedite their examination, the Applicants, rather than re-writing their prior claims, have simply canceled all the prior claims 1-14 and substituted new claims 15-30 there for.

New 15-30 claims have been drafted to define the invention with increased precision.

To facilitate examination, the following table shows the correspondence between the prior claims 1-14 and new claims 15-30.

Present Claim	Prior Claim	Present Claim	Prior Claim
15	1	23	9
16	2	24	10
17	3	25	11
18	4	26	None
19	5	27	None
20	6	28	12
21	7	29	13
22	8	30	14

As indicated, each of new dependent claims 26 and 27, both of which directly depend from independent claim 15, has no counterpart in any of the prior claims.

Rejections

A. Rejection under 35 USC § 102

The Examiner has rejected prior claims 1-10 and 12-14, under the provisions of 35 USC § 102(b) as being anticipated by the teachings of the Atkinson et al patent (United States patent 5,892,904 issued to R. G. Atkinson et al on April 6, 1999). Inasmuch as all these claims have now been canceled, this rejection is moot. Nevertheless, since these claims have been replaced by new corresponding claims 15-24 and 28-30, this rejection will be discussed in that context and principally with respect to new independent claim 15. In that context, this rejection is respectfully traversed.

In essence, the Examiner takes the position that the Atkinson et al patent identically discloses all the features of all the prior claims. As the Examiner will soon appreciate this view is incorrect with respect to claim 15 (as well as all the other independent claims).

Specifically and as discussed in col. 2, line 34 et seq of the Atkinson et al patent, that patent discloses a method for ensuring authenticity and integrity of a computer program. Through use of the method, a software publisher or distributor can "sign" an executable file with a digital signature so that the file can then be transmitted with confidence over an open network, such as the Internet, to a recipient client computer. What this method assures to the recipient is that the file, once signed, is, as expressly stated in col. 2, lines 43-48 of this patent: (a) the identity of the publisher, i.e., that the file is "authentic" in that it originates from that publisher, and (b) that the file has not been modified after it has been transmitted by the publisher to the recipient. The patent specifically defines the term "integrity" as referencing a file that "has not been modified after being transmitted by the publisher". In effect, that is from the time the file has left the publisher to the time it is received by its recipient, the file has not been changed, whether by, e.g., a transmission artifact or by an intentional or other act undertaken by a third-person or machine. Use of such a signature, implemented through employing a digital certificate, forms the basis of, e.g., the Microsoft "Authenticode" method.

Conventional methods of this sort, as discussed on page 1, lines 15-22 of the present application, are problematic. Specifically, the signature, when affixed to a software component, provides absolutely no guarantee or certification that the component will provide certain functionality, let alone that the functionality is correctly implemented. All that the signature, taught by the Atkinson et al patent, would indicate is that the software component, regardless of whatever functionality it contains, was communicated in an error-free manner from the party who supplied the component and its signature, e.g., a manufacturer or distributor, to its recipient, e.g., an end-user. If, illustratively, that component were to include a virus or other pernicious computer code, embedded by the component manufacturer, and then the manufacturer affixed the signature to the component, then the signature would never reflect the addition of the code and hence, at least from the signature itself, the user would not be aware of that code and obviously any risk the component poses.

The present Applicants describe a method and apparatus for distributing software components which eliminates those drawbacks.

In sharp contrast to the express teachings of the Atkinson et al patent, the Applicant's view of "integrity" differs diametrically from the meaning of that term as defined in that patent.

In particular, as described in the present application at, e.g., page 2, line 35 through page 3, line 6; page 4, lines 3-5 and 23-28; page 5, lines 22-25; and page 6, lines 15-16, the Applicants teach an inventive process, of distributing a software component, which relies on creating integrity test data from that component and creating an integrity certificate containing that test data. The integrity data reflects the functionality provided by that component and the quality of that component. This certificate would preferably be created by a third-party certificate originator, independent of the software manufacturer, and then provided to a user's client computer which, typically via a download, has received the component from its manufacturer or distributor. A user at that computer can then check the certificate to determine proper version, functionality, quality, security, etc all as specified by the software manufacturer. From the data contained in the certificate, the user can determine whether the component will meet that user's demands with respect to quality and/or functionality.

Consequently, as the Examiner can appreciate, the integrity data itself, as described by the present Applicants, has *no* bearing as to whether the software component has been modified after its transmission to a recipient. However, if that software component were inherently to poorly function and/or exhibit inferior quality -- such as by including pernicious or other problematic software code, then the integrity data for the component would reflect that fact. In contrast, the digital signature taught by the Atkinson et al patent *would not.* Thus, a user who has downloaded the component and obtained a integrity certificate for that component, as taught by the present Applicants, could then by viewing information reflected in that data be advised of such problems prior to installing that software. In contrast, the user *could not* do that using the methodology taught by the Atkinson et al patent and thus would remain completely oblivious to that situation, and any risk it posed, until after the software was installed -- when it might be too late to avoid damage or expense.

Independent claim 15 of the present application contains suitable recitations directed to the distinguishing aspects of the present invention. In particular, this claim recites as follows, with those distinguishing recitations shown in a bolded typeface:

> "A method for distributing software components, the method comprising the steps of:
>
> deriving a first software component identifier from a software component;
>
> **creating integrity test data by performing, on the software component, an integrity test relating to at least one of the quality and the functionality of the software component;**
>
> **creating, by an integrity certificate originator and using the first software component identifier, an integrity certificate having the integrity test data;**
>
> retrieving the software component through a client computer;
>
> deriving, by the client computer, a second software component identifier from the software component;
>
> **retrieving the integrity certificate by the client computer and using the second software component identifier;** and
>
> **disclosing the integrity test data to a user by the client computer."** [emphasis added]

Each of the other new independent claims 28-30 contains distinguishing limitations which are quite similar to those appearing in claim 15.

Since the recited features of creating integrity test data for a software component, the data reflecting quality and/or functionality of that component, and its use in conjunction with an integrity certificate are not disclosed, taught or shown in the Atkinson et al patent, then each of these independent claims is not anticipated by the teachings of that patent.

Hence, the Applicants submit that all of these independent claims are patentable under the provisions of 35 USC § 102(b).

Each of dependent claims 16-25 directly or indirectly depends from independent claim 15 and recites a further distinguishing aspect(s) of the present invention from those recited in that independent claim. As such, the Applicant submits that each of these dependent claims is also not anticipated by the teachings of the Atkinson et al patent for the same reasons set forth above with respect to independent claim 15. Consequently, each of dependent claims 16-25 is also patentable under the provisions of 35 USC § 102(b).

Consequently, this rejection should now be withdrawn.

B. Rejection under 35 USC § 103

The Examiner has rejected prior dependent claim 11, under the provisions of 35 USC § 103, as being obvious over the teachings of the Atkinson et al patent taken in view of those in the Shetty et al patent (United States patent 6,799,197 issued to S. Shetty et al on September 28, 2004). Inasmuch as this claim has also been canceled, this rejection is moot as well. Nevertheless, since this claim has been replaced by new corresponding dependent claim 25, this rejection will be discussed in that context and principally with respect to new independent claim 15 from which claim 25 directly depends. In that context, this rejection is also respectfully traversed.

The Examiner cited to the Shetty et al patent for its apparent teaching of providing an email distribution capability. The feature of distributing integrity certificates by email was recited in prior claim 11.

In particular, the Shetty et al patent is directed to a method and system for securely administering software installed on a number of client computers. In essence, policies are defined for one or more such computers and stored on and securely transmitted from a server, under control of a system administrator, to each of the clients. The policy may itself contain software configurations for software that resides on the clients, software to be installed on the clients, or other information and data that is needed to maintain and manage the clients. The policy is contained with an information package assembled by and stored on a server and subsequently securely transmitted, through, e.g., email, to each client computer. See abstract, and col. 2, line 38 et seq of the Shetty et al patent.

As to security of each package, this patent states in col. 6, lines 50-52, that each package is digitally signed by the entity that created it and may be encrypted as well. Presumably, the certificate is used, in accordance with conventional teachings, such as the previously described "Authenticode" methodology, merely to authenticate the source package and assure that the package has not been modified during transmission from the server to a recipient client.

Nowhere does the Shetty et al patent contain any teachings, whether express or implicit, concerning the Applicants' present inventive concept of incorporating or using a digital certificate that contains integrity data, with that data reflecting functionality and/or quality of a corresponding software component that has been distributed to a client computer.

Hence, any combination of the teachings in the Atkinson et al and Shetty et al patents would result in the very same deficiencies, as described above, that exist in the Atkinson et al patent alone. Thus, no one skilled in the art, when faced with the teachings in both of these patents would be led any closer to the Applicants' present invention than were that person to be faced with the limited teachings in Atkinson et al patent taken alone.

Consequently, independent claim 15 is not obvious over the teachings in the Atkinson et al and Shetty et al patents, whether those patents are viewed singly or their teachings combined in any manner, including that posed by the Examiner. Thus, claim 15 is patentable under the provisions of 35 USC § 103.

Claim 25, which corresponds to prior claim 11, directly depends from independent claim 15 and recites a further distinguishing aspect of the present invention from those recited in that independent claim. As such, claim 25 is also not rendered obvious over the teachings of the Atkinson et al and Shetty et al patents for the same reasons set forth above with respect to independent claim 15. Consequently, dependent claim 25 is also patentable under the provisions of 35 USC § 103.

Hence, this rejection should also now be withdrawn.

Conclusion

Thus, the Applicants submit that none of the claims, presently in the application, is either anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103.

Consequently, the Applicants believe that all these claims are presently in condition for allowance.

OIPE
IAP87
DEC 16 2008
PATENT & TRADEMARK OFFICE

Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

December 12, 2008

Peter L Michaelson

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 542-7800

MICHAELSON & ASSOCIATES
Counselors at Law
P.O. Box 8489
Red Bank, New Jersey 07701-8489

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **December 12, 2008** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Peter L Michaelson

Signature

30,090
Reg. No.